UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/057,066	01/25/2002	Sihai Xiao	TVW/APP35US	5026

59906   7590   10/05/2007
SYNNESVEDT & LECHNER, LLP
TVWORKS, LLC
1101 MARKET STREET
SUITE 2600
PHILADELPHIA, PA 19107

EXAMINER
PICH, PONNOREAY

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
10/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/057,066	XIAO, SIHAI
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 September 2007*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22, 24, 29-37 and 50-55* is/are pending in the application.

  4a) Of the above claim(s) *7-13 and 31-37* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6, 14-22, 24, 29-30, 50-55* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

  Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

  Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

  a)☐ All b)☐ Some * c)☐ None of:

    1.☐ Certified copies of the priority documents have been received.

    2.☐ Certified copies of the priority documents have been received in Application No. _____.

    3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

  * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application
6)☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9/10/07 has been entered.

Claims 1-6, 14-22, 24, 29-30, and 50-55 were examined. Well known art statements made in the last office action not specifically or adequately traversed are taken as admittance of prior art as per MPEP 2144.03.

Response to Arguments

Applicant's arguments with respect to the amended claims were fully considered. Applicant notes that Hericourt fails to disclose <u>transmitting a TIO from a server to a client to facilitate validation</u>. Applicant states that the CAF tables 310 (which could be interpreted as a TIO) containing the certificate data are disclosed by Hericourt as being maintained by a security administrator and is resident in the client devices, thus the claims as amended overcomes Hericourt's teachings under 35 USC 102. Applicant also states that it would not be obvious to modify the CAF tables as disclosed by Hericourt such that it, i.e. the TIO, is downloadable into a client, thus the claims as amended also overcomes Hericourt under 35 USC 103. Applicant states that since the devices are already configured to accommodate the tables, there is little reason to

modify Hericourt's devices such that the tables are eliminated and are instead downloaded.

The examiner agrees that the claims as amended overcome Hericourt's teachings under 35 USC 102 because Hericourt does not explicitly disclose transmitting/downloading a TIO, i.e. the CAF table, from a server to a client. However, the examiner respectfully disagrees that it would have been unobvious to modify Hericourt's teachings such that the tables are downloaded into the devices. As recognized by applicant, the CAF tables are maintained by a security administrator. However, it should also be recognized that Hericourt silent with respect to how the security administrator maintains the CAF table located in device 308 as seen in Figure 3, thus Hericourt dislcoses an invention that is ready for improvement. A person of ordinary skill would readily recognize that in an administrator might maintain the table in several manners. First, one skilled should recognize that device 308 must obtain the table in some manner for it to have a table. Some ways that comes to mind is that the tables could be preprogrammed into the devices and the administrator only has to update the tables or the tables are in fact installed into the device 308 by the administrator. The administrator could do such installation at the device itself or could download the table into the device. As is explained further below, the downloading of a TIO to a client by a security administrator was well known in the art. As such, incorporating such teachings within Hericourt's invention would do no more than yield the predictable result of a device 308 having a CAF table installed into a client by a security administrator.

Claim Objections

Claims 1, 52-55, and 15 are objected to because of the following informalities:

1. The second limitation of claim 1 should recite "verifying said received certificate..." since a received certificate is already recited in the preamble of the claim.

2. The number 52 is used to number two different claims in the current application. The examiner will assume that the second claim 52 is meant to be claim 53 and claims 53-55 should instead be claims 54-56 respectively.

3. "said certificate" in line 3 of claim 15 should be "said signing certificate".

4. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 2 and 53 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. "said trust entity certificates" as recited in line 4 of claim 2 appears to lack antecedent basis.

2. Because the number 52 is used to number two different claims, it is unclear to which claim the claim that is currently numbered as claim 53 is supposed to refer—the first claim 52 or the second.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 22, 24, and 29-20 are rejected under 35 U.S.C. 102(b) as being

anticipated by Micali (US 5,717,757).

Claims 1 and 22:

As per claim 1, Micali discloses:

1. Downloading a trust information object (TIO), i.e. certificate issue list (CIL), from

a server to said memory of said client (col 7, lines 4-12; col 8, lines 6-8; and col

10, lines 28-31), said TIO comprising at least a plurality of hash values, each

hash values being hashed from a trust entity certificate (col 6, lines 47-54; col 7,

lines 13-27; and col 9, line 65-col 10, line13), and a plurality of trust vectors, each

trust vector corresponding to a hash value and being indicative of the level of

trust associated with a particular entity certificate (col 7, lines 43-59 and col 9,

lines 46-49). *Note that as the examiner is interpreting the CIL disclosed by Micali*

as being a TIO. Micali discloses that a certificate authority (CA) creates the CIL.

An intermediary receives the CIL and can further forward the CIL to others. The

CIL itself is disclosed in many embodiments. In one embodiment, it could

contain a plurality of hash values obtained by hashing certificates and also

containing information related to the validity of the certificates, which the

examiner is interpreting as trust vectors.

2. Verifying said received certificate by hashing said received certificate to generate

   a resulting hash value, comparing said resulting hash value to said hash values

   in said TIO to determine if a match exists, and if said match is found, determining

   if the corresponding trust vector indicates requisite level of trust to establish

   connection (col 5, lines 40-42; col 9, lines 39-42; col 9, line 65-col 10, line 13;

   and col 10, lines 35-42). *An intermediary could be sent an entire certificate to*

   verify the status of the certificate, i.e. determine its trust vector. Micali discloses

   that one way to verify the certificate is to hash the certificate and compare the

   hash value to a hash value on hand, i.e. stored in the CIL. Information regarding

   the status of the certificate (i.e. if it is issued, revoked, valid, etc.) is sent back to

   the user who sent the certificate to the intermediary for verification.

   Claim 22 is directed towards an apparatus for performing the method of claim 1

and is rejected for much the same reasons as claim 1. The examiner considers the

intermediary disclosed by Micali as being the client device recited in claim 22.

Claims 24 and 29-30:

   Claim 24 and 29-30 appear to further define the TIO (i.e. a material worked on by

the claimed apparatus) rather than the claimed apparatus. Because an apparatus's

patentability depends on its structure rather than any material worked on by the

apparatus (see MPEP 2114), it does not appear that what is further recited in claims 24

and 29-30 further define the apparatus claimed in claim 22 and as such claims 24 and

29-30 are rejected for the same reasons as those discussed in claim 22.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 22, 50-54, 56, 24, and 29-30 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Hericourt et al (US 2002/0078347) in view of Samar (US

6,304,974) in further view of Micali (US 5,717,757).

Claims 1 and 22:

Hericourt discloses a TIO (Fig 5), i.e. CAF Table, comprising at least a plurality of

hash values, each hash value being hashed from a trusted entity certificate (paragraphs

11, 17, 135 and Fig 4, item 504), and a plurality of trust vectors, each trust vector

corresponding to a hash value and being indicative of the level of trust associated with a

particular trusted entity certificate (paragraphs 135 and 138-141 and Fig 4, item 507).

The examiner is interpreting the CAF table as seen in device 308 (see Fig 3) as a TIO.

The table contains a plurality of records related to CA certificates. As discussed in

paragraphs 11 and 17 a certificate could contain such information as a hash value of

the certificate itself. Note that Hericourt does not place any limits on the type of

certificates that could be used in his invention. As seen in Figure 5, each record in the

table contains the certificate itself, thus the CAF table contains a plurality of hash values

hashed from the CA certificate since each certificate contain its own hash. Each record

also contains a CA_Trust_Level 507, which the examiner is interpreting as a trust

vector. Because there are multiple records, there is a plurality of trust vectors in the

CAF table, each vector corresponding to the certificate and hash value. Hericourt also

discloses verifying a received certificate (paragraph 104).

Hericourt does not explicitly disclose of downloading a trust information object

(TIO) from a server to said memory of said client. In fact, Hericourt does not discuss at

all how device 308 obtained the CAF table, i.e. the TIO. Hericourt discloses that a

security administrator periodically maintains the CAF table (paragraph 135). However,

because Hericourt does not explicitly explain how the administrator maintains the table

one of ordinary skill would recognize that the Hericourt's invention is one which is ready

for improvement and one in which one of ordinary skill could apply a variety of known

table maintenance techniques to achieve the table maintenance. Samar discloses one

manner in which a table is provided to a client is by downloading the table to the client

by an administrator (col 8, lines 20-39). It would have been obvious to one of ordinary

skill in the art at the time applicant's invention was made to incorporate Samar's

teachings within Hericourt's invention. One skilled would do so by having Hericourt's

security administrator create a CAF table and download the table from the

administrator's computer, i.e. a server, to a device 308's memory, i.e. a client's memory.

The rationale for why it would have been obvious for one of ordinary skill to do this in

light of Samar's teachings is that Hericourt's invention is one which is ready for

improvement since he does not explicitly teach how a security administrator maintains

the CAF table in device 308 and how device 308 obtained the table in the first place.

The application of Samar's teachings within Hericourt's invention does no more than

yield a predictable result of the security administrator maintaining the CAF table via

delivery of the table from a server to a client's memory, i.e. delivery from the

administrator's computer to device 308's memory.

Hericourt also does not explicitly disclose verifying a received certificate by

hashing said received certificate to generate a resulting hash value, comparing said

resulting hash value to said hash values in said TIO to determine if a match exists, and

if said match is found, determining if the corresponding trust vector indicates requisite

level of trust to establish connection. However, the limitation is disclosed by Micali (col

5, lines 40-42; col 9, lines 39-42; col 9, line 65-col 10, line 13; and col 10, lines 35-42).

At the time applicant's invention was made, it would have been obvious to one of

ordinary skill in the art to further modify Hericourt's invention using Micali's teachings

according to the limitations as recited in claim 1. One of ordinary skill would have been

motivated to verify a certificate according to Micali's teachings because as recognized

by Micali, hashes produce fewer bits (col 10, lines 19-20), thus comparison for purposes

of verification would be faster via use of hashes rather than comparing the entire

certificate.

Note that with respect to the present application, the examiner has determined

that a person of ordinary skill in the art is someone having at least MS in Computer

Science and specializing in cryptography (or someone with equivalent industry

experience).

Claim 22 is directed towards an apparatus for performing the method of claim 1

and is rejected for much the same reasons as claim 1. The examiner considers device

308 of Hericourt as being the client device recited in claim 22.

Claim 50:

Samar further discloses wherein said TIO is updated periodically by said TIO-

provider server (col 8, lines 20-39). The list disclosed by Samar in the cited section is

similar to the CAF table of Hericourt because it is used to keep track of certificates, thus

can also be considered a TIO. As such, the techniques used with the list of Samar

could be applied to any type of TIO.

Claim 51:

Hericourt does not explicitly disclose wherein downloading said TIO comprises

broadcasting said TIO. However, official notice is taken that broadcasting data to

clients as a way of data delivery was well known in the art at the time applicant's

invention was made. It would have been obvious to one of ordinary skill in the art to

further modify Hericourt invention such that downloading said TIO comprises

broadcasting said TIO. One of ordinary skill would have been motivated to do so

because broadcasting is a quick way of distributing data to a large number of clients.

Note that in Hericourt's invention, there are multiple device 308, thus a way to distribute

information to all the devices at the same time would be useful in Hericourt's modified

invention.

Claim 52:

Micali further discloses wherein said TIO is signed (col 6, lines 55-56).

Claim 53:

Micali further discloses wherein said TIO is downloaded each time a received

certificate is verified (col 8, lines 60-67 and col 10, lines 29-32).

Claim 54:

Hericourt does not explicitly disclose wherein said TIO is cached in memory.

However, official notice is taken that caching data in memory was well known in the art

at the time applicant's invention was made. It would have been obvious to one of

ordinary skill in the art to further modify Hericourt's invention such that said TIO is

cached in memory. One skilled would have been motivated to do so because it would

speed up processing when a TIO needs to be accessed. Data is typically cached in a

computer system to speed up processing.

Claim 56:

Hericourt does not explicitly disclose wherein TIO is downloaded using one of

broadcast or http. However official notice is taken that broadcast and http were both

well known methods of downloading data at the time applicant's invention was made. It

would have been obvious to one of ordinary skill in the art to further modify Hericourt's

invention such that the TIO is downloaded using one of broadcast or http. One skilled

would have been motivated to do so because both were commonly used forms of data

distribution at the time applicant's invention was made. Modifying Hericourt's invention

such that broadcast or http was used to download TIO would do no more than yield a predictable result.

Claims 24 and 29-30:

Claim 24 and 29-30 appear to further define the TIO (i.e. a material worked on by the claimed apparatus) rather than the claimed apparatus. Because an apparatus's patentability depends on its structure rather than any material worked on by the apparatus (see MPEP 2114), it does not appear that what is further recited in claims 24 and 29-30 further define the apparatus claimed in claim 22 and as such claims 24 and 29-30 are rejected for the same reasons as those discussed in claim 22.

Claims 2 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hericourt et al (US 2002/0078347) in view of Samar (US 6,304,974) in further view of Micali (US 5,717,757) in further view of Hsu et al (US 5,982,898).

Claims 2 and 24:

As per claims 2 and 24, Micali discloses wherein said TIO further comprises a timestamp of when said TIO is created (col 6, lines 40-41). Note the CIL disclosed by Micali serves a similar function as the CAF table disclosed by Hericourt and could also be considered a TIO. Micali also discloses said TIO further comprises a digital signature of all data in the TIO included in said TIO (col 6, lines 55-61).

Hericourt, Samar, and Micali do not explicitly disclose said TIO comprises a value indicating a number of signatures required for a next update. However, the

limitation is disclosed by Hsu (col 5, lines 29-37, i.e. the number of times a certificate can be used before expiring/requiring an update).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to also include a number of signatures required for a next update as part of a TIO. One skilled would have been motivated to do so because it would provide for a way to ensure the TIO is updated regularly, thereby ensuring the TIO contains up-to-date information about issued certificates. Note that as per Micali's teachings, the digital signature is of the entire TIO, thus if a value indicating a number of signatures required for a next update is included as part of the TIO, the digital signature would include said trust entity certificates, said number of signatures, and said timestamp.

Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hericourt et al (US 2002/0078347) in view of Samar (US 6,304,974) in further view of Micali (US 5,717,757) in further view of Vogel et al (US 6,816,900).

Claim 3:

Hericourt does not explicitly disclose wherein said hash value is determined using any of MD5 and SHA-1. However, Vogel discloses wherein a hash value is determined using any of MD5 and SHA-1 (col 7, lines 45-63).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify Hericourt's invention such that said hash value is determined using any of MD5 and SHA-1. One skilled would have been motivated to do so because both MD5 and SHA-1 are conventional ways of obtaining hash values for signatures.

Claim 4:

Hericourt does not explicitly disclose wherein said TIO conforms to the PKCS#7 standard. However, Vogel discloses the PKCS#7 standard being used to sign messages (col 7, lines 37-44). At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify Hericourt's invention such that said TIO conforms to the PKCS#7 standard. One skilled would have been motivated to do so because PKCS#7 offers a high level of security and is the standard for signing messages using certificates under a PKI. Hericourt discloses messages signed via certificates (paragraph 76).

Claims 5-6, 30, and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hericourt et al (US 2002/0078347) in view of Samar (US 6,304,974) in further view of Micali (US 5,717,757) in further view of applicant's admittance of prior art, herein referred to as AAPA.

Claim 5:

Hericourt does not explicitly disclose hard coding said TIO into said client's software. However, AAPA discloses that at the time applicant's was made, it was a common approach in the art to hard code a TIO into a client's software (specification, page 2, lines 4-6).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill to further modify Hericourt's invention by hard coding a TIO into said client's software. One of ordinary skill would have been motivated to hard code a TIO into a client's software because as applicant discloses in the specification, it was a common approach in the art to provide associated trust information (specification, p2, lines 4-6).

Claims 6 and 30:

Hericourt does not explicitly disclose saving a copy of said TIO in persistent memory during said client's build time. However, this limitation is disclosed by AAPA as it was discussed as being well known in the art in prior office actions.

At the time applicant's invention was made, it would have been obvious to further modify Hericourt's invention such that a copy of the TIO was saved in a persistent memory during said client's build time. One of ordinary skill would have been motivated to do so because it was common to assign trust information to a client during build time and to save it in persistent memory to prevent lost of the information due to power.

Claim 55:

Hericourt does not explicitly disclose wherein said TIO is stored in persistent memory. However, as discussed in claim 6, storing TIO in persistent memory was

discussed by AAPA as being well known in the art. It would have been obvious to one

of ordinary skill in the art to further modify Hericourt's invention such that said TIO is

stored in persistent memory for the same reasons and motivations given in claim 6.

Claims 14-17 and 20-21 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Hericourt et al (US 2002/0078347) in view of Samar (US 6,304,974).

Claim 14: .

Hericourt discloses a TIO (Fig 5), i.e. CAF Table, comprising at least a plurality of

hash values, each hash value being hashed from a trusted entity certificate (paragraphs

11, 17, 135 and Fig 4, item 504), and a plurality of trust vectors, each trust vector

corresponding to a hash value and being indicative of the level of trust associated with a

particular trusted entity certificate (paragraphs 135 and 138-141 and Fig 4, item 507).

The examiner is interpreting the CAF table as seen in device 308 (see Fig 3) as a TIO.

The table contains a plurality of records related to CA certificates. As discussed in

paragraphs 11 and 17 a certificate could contain such information as a hash value of

the certificate itself. Note that Hericourt does not place any limits on the type of

certificates that could be used in his invention. As seen in Figure 5, each record in the

table contains the certificate itself, thus the CAF table contains a plurality of hash values

hashed from the CA certificate since each certificate contain its own hash. Each record

also contains a CA_Trust_Level 507, which the examiner is interpreting as a trust

vector. Because there are multiple records, there is a plurality of trust vectors in the

CAF table, each vector corresponding to the certificate and hash value. Hericourt also discloses verifying a received certificate (paragraph 104).

Hericourt does not explicitly disclose of downloading a trust information object (TIO) from a server to said memory of said client. In fact, Hericourt does not discuss at all how device 308 obtained the CAF table, i.e. the TIO. Hericourt discloses that a security administrator periodically maintains the CAF table (paragraph 135). However, because Hericourt does not explicitly explain how the administrator maintains the table one of ordinary skill would recognize that the Hericourt's invention is one which is ready for improvement and one in which one of ordinary skill could apply a variety of known table maintenance techniques to achieve the table maintenance. Samar discloses one manner in which a table is provided to a client is by downloading the table to the client by an administrator (col 8, lines 20-39). It would have been obvious to one of ordinary skill in the art at the time applicant's invention was made to incorporate Samar's teachings within Hericourt's invention. One skilled would do so by having Hericourt's security administrator create a CAF table and download the table from the administrator's computer, i.e. a server, to a device 308's memory, i.e. a client's memory. The rationale for why it would have been obvious for one of ordinary skill to do this in light of Samar's teachings is that Hericourt's invention is one which is ready for improvement since he does not explicitly teach how a security administrator maintains the CAF table in device 308 and how device 308 obtained the table in the first place. The application of Samar's teachings within Hericourt's invention does no more than yield a predictable result of the security administrator maintaining the CAF table via

delivery of the table from a server to a client's memory, i.e. delivery from the administrator's computer to device 308's memory.

As per the limitations of said client periodically connecting to said server to determine whether a new TIO is available; and said server sending a new to said client if said new TIO is available, the limitations are disclosed by Samar (col 8, lines 20-44), thus are obvious to Hericourt and Samar's combination invention.

Claim 15:

Hericourt and Samar renders obvious all the limitations recited in claim 14. Further, Samar discloses sending said TIO with a signing certificate to said client, wherein trust information of said signing certificates indicates that said signing certificate can be trusted for signing said TIO (col 3, lines 4-13).

Claim 16:

Hericourt and Samar renders obvious all the limitations recited in claim 14. Samar further discloses wherein said client fetches said TIO from a trusted server, said client ensuring that a root certificate that signed said signing certificate is contained in said TIO (Fig 5).

Samar does not disclose said root certificate is not revocable. However, the examiner asserts that non-revocable certificates were well known in the art at the time applicant's invention was made. It would have been obvious to one of ordinary skill in the art to further modify Hericourt's invention such that the root certificate was not revocable because it would indicate a high level of trust for the user of the root certificate.

Claim 17:

Hericourt and Samar renders obvious all the limitations recited in claim 14.

Samar further discloses wherein said client verifies a digital signature of said TIO with a

signing certificate, along with a TIO sent to said client (col 5, lines 46-51 and col 7, lines

17-23).

Claim 20:

Hericourt and Samar renders obvious all the limitations recited in claim 14.

Hericourt does not explicitly disclose wherein said TIO is delivered to said client via a

broadcast channel; wherein a provider delivers an initial TIO to said client that contains

a signing certificate and associated trust information by either of including said signing

certificate in the initial TIO saved in a client persistent memory, or by sending the initial

TIO to said client through a secure channel before using said broadcast channel.

However, the examiner asserts that the limitation is well known in the art, as

discussed in a prior office action. At the time applicant's invention was made, it would

have been obvious to one of ordinary skill to further modify Hericourt's invention to use

a broadcast channel as recited in claim 20. One skilled would have been motivated to

do so because sending a TIO via a broadcast channel is the quickest and cheapest way

of distributing the same information to a large group of clients. One of ordinary skill

would have been motivated to deliver an initial TIO to the client via a secure channel

before using a broadcast channel as this would initially ensure that only authorized

clients received subsequent TIO's.

Claim 21:

Hericourt and Samar renders obvious all the limitations recited in claim 14.
Hericourt does not explicitly disclose updating said TIO on a per session basis when
said TIO is not persistently stored. However, as discussed in the prior office action, this
limitation was well known in the art at the time applicant's invention was made. It would
have been obvious to one skilled to have further modified Hericourt's invention
according to the limitations recited in claim 21. One skilled would have been motivated
to do so because it would prevent untrustworthy certificates from being used.

Claims 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over
Hericourt et al (US 2002/0078347) in view of Samar (US 6,304,974) and further in view
of Vogel et al (US 6,816,900).

Claim 18:

Hericourt and Samar renders obvious all the limitations recited in claim 17.
Hericourt does not explicitly disclose wherein multiple signatures are verified, depending
on the number of signatures specified in said TIO; wherein said client hashes said
signing certificates one by one; and wherein if proper results are found in said TIO and
said certificates are trusted for signing said TIO, then said TIO proves that it was not
tampered with.

However, Vogel discloses wherein multiple signatures are verified, depending on
the number of signatures specified in a TIO (col 8, lines 9-17). Vogel also does not
explicitly disclose wherein if proper results are found in said TIO and said certificates

are trusted for signing said TIO, then said TIO proves that it was not tampered with. However, the purposes of signatures are to verify and validate. If proper results are found for the signatures, then by definition, the TIO has proven that it was not tampered with.

It would have been obvious to one of ordinary skill to further modify Hericourt's invention according to the limitation recited in claim 18 in light of Vogel's teachings because it would allow one to determine which CA's are no longer trustworthy due to possible security breaches. Note Hericourt discloses wanting to remove untrustworthy CA's from the list of trusted CA's (paragraphs 136-137).

Claim 19:

Hericourt and Samar renders obvious all the limitations recited in claim 19. Hericourt does not explicitly disclose wherein said signing certificates exist in said TIO in said client before said TIO is signed. However, official notice is taken that at the time applicant's invention was made, it was well known for a client to receive and store a signing certificate from a CA before messages signed with the certificate is sent to the client. In light of this, it would have been obvious for one skilled to have further modify Hericourt's invention according to the limitations recited in claim 19. One skilled would have been motivated to do so because it would allow a client to quickly verify the authenticity of a message/response/TIO received if the client already had the signing certificate with which it can perform authentication of a signature.

Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Hericourt et al (US 2002/0078347) in view of applicant's admittance of prior art, herein

AAPA, and further in view of Vogel et al (US 6,816,900).

Claim 29:

Hericourt does not explicitly disclose wherein said TIO comprises a TIO derived

from a set of root certificate authority (CA) certificates hard coded into a software of said

client device. However, AAPA discloses that at the time applicant's was made, it was a

common approach in the art to hard code a TIO into a client's software (specification,

page 2, lines 4-6). Further, the examiner asserts that it was well known to derive a TIO

from a set of root CA certificates. This is further evidenced by Vogel (col 4, lines 5-37).

At the time applicant's invention was made, it would have been obvious to one of

ordinary skill to further modify Hericourt's invention by hard coding a TIO derived from a

set of root CA certificates into said client's software. One of ordinary skill would have

been motivated to hard code a TIO into a client's software because as applicant

discloses in the specification, it was a common approach in the art to provide

associated trust information (specification, p2, lines 4-6). One skilled would have been

motivated to derive a TIO from a set of root CA certificates because it would offer a high

level of security for the certificate in the TIO since the certificate would be verified by a
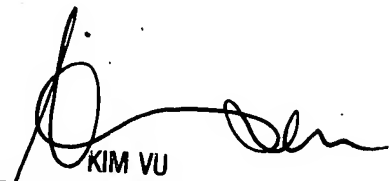
chain of CA's.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ponnoreay Pich
Examiner
Art Unit 2135

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100